Research on Big Data Security Privacy Protection Based on Cloud Computing

Liu Guangjun*, Yang Weiqing, Zhan Lining, Li Xiangjun

School of Information Engineering, Xi’an University, Shaanxi, Xi’an, 710065, China

*corresponding author

Keywords: Cloud Computing, Big Data Security, Privacy Protection

Abstract: With the continuous development of information technology, the integrated use of big data realized by cloud computing makes people's life more convenient and fast. at the same time, the potential security hidden danger when big data is used brings a lot of troubles to people, and even brings mental damage and economic losses. Therefore, the security privacy protection of big data has become the focus of the current research, this paper starts from the analysis of the security problems faced by cloud computing, deeply analyzes the causes of security problems, and puts forward corresponding protection strategies for these problems.

1. Introduction

At present, big data technology has been widely used in various industries, which has a profound impact on the economic development of our country. Through cloud computing, tens of thousands of data processing can be completed quickly in a few seconds, realizing the full sharing of resources, because of the cloud computing data is very large, diffuse, ubiquitous distribution and sociality [1]. Therefore, how to solve these problems is of great significance.

2. Security Privacy Threats Based on Cloud Computing

Although cloud computing has become a mainstream delivery option for applications, services and infrastructure, there are still concerns about cloud security. According to relevant reports, the security problems faced by cloud computing are mainly focused on virtualization security, data security, network security and security of confidentiality, as shown in figure 1.

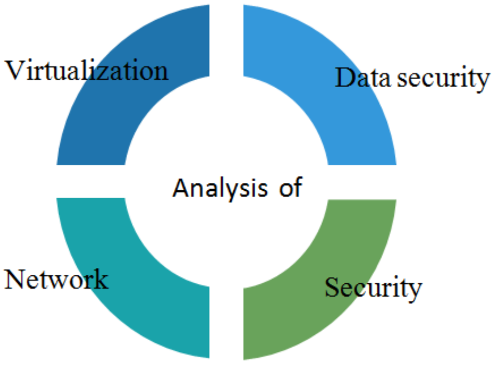

Figure 1 Safety privacy pain point analysis

2.1. Virtualization Security Privacy Threats

Virtualization is the meaning of cloud computing, the two complement each other in technology, virtualization technology can make cloud computing applications more flexible, and bring users a better service experience. However, the application of virtualization technology also makes cloud computing security technology higher, because virtual machines can be created and migrated arbitrarily in the two-tier network, and the security measures made by virtual machines are difficult to create and migrate, especially the migration is more difficult. In this case, virtual machines can

DOI: 10.25236/cseem.2020.162

easily lead to key loss, cloud policy services are attacked, weak password, no password theft and so on.

2.2. Data Security Privacy Threats

Cloud computing is distributed in the computing resources of the massive data analysis and calculation, completed together, and finally aggregated to the cloud, a large amount of data transmission through the network this process is no protection, so there is a great security risks. Similarly, there is a security threat to the storage side of the data, although the data stored in the cloud can be encrypted and saved, and the key is stored in the client, which seems to be very secure. Once the hacker carries on the network attack and encrypts the cloud data, the key in the hands of the network attacker will pose a great threat to the cloud data security. In addition, when the user exits the data stored in the cloud, if the data space is not cleaned up in time, the data will likely be stolen by other users, and there is also the possibility of data disclosure.

2.3. Network Security Privacy Threats

Compared with traditional computing methods, cloud computing must have ready access to the network for easier user use, resulting in distributed cloud resource network architecture, more complex distributed management of network devices, and more vulnerable to network hacking, not only from external networks, but also from internal networks, such as IaaS and DDoS. In addition, some malicious attacks in traditional networks are also present in cloud computing environments (such as ARP attacks), and their risk levels will multiply.

2.4. Identity Authentication Security Privacy Threats

Big data in cloud computing comes from massive users. In order for users to get efficient and fast service experience, the authentication process of user's identity authentication and docking management is very simple. At present, e-commerce has become a kind of new business mode, whether it is daily goods or valuable objects, it can be traded through the network. In order to realize users'access to cloud computing from different locations and different clients, the general authentication is to use the single sign-on mode of using the business to use the unified single sign-on mode.

3. Causes of Big Data Security Threats

Macroscopically, big data security threats can be divided into natural threats and man-made threats [2]. Two parts. Natural threats come from natural disasters, electromagnetic radiation and interference, network equipment aging and other force majeure, but need to strengthen prevention is from human malicious or unintentional damage, as well as malware illegal intrusion and other formation of human threats, for passive attacks derived from human attacks, the focus of prevention is prevention; and for active attacks, the focus is on detection and recovery.

4. Research on Security Privacy Protection of Big Data

From the above analysis, we can see that cloud computing unconsciously changes our lives, and similarly, the security of cloud computing also needs new technical support to make it more secure and stable service for us. While traditional security tools aren't for big data security, more than half of companies choose to train in-house IT personnel to address security issues, while about a third invest more in the budget for cloud security, according to research.

4.1. Large Data Security Safeguards

The big data security model is shown in figure 2, through the platform operation audit, export review, access control [3] equal multiple security protection barrier big data for security protection. First of all, the big data knowledge base sensitivity assessment and data desensitization, in data extraction and integration, data need to be desensitized, cleaned, to ensure that the data involved in privacy will not be extracted; on the other hand, the data extractor identity authentication control, two-pronged approach to ensure the privacy of big data security. Throughout the whole life cycle of big data, big data from the data source to the whole process of being applied, through the platform facilities security, interface security, data security, application security and system layer security to form a comprehensive security guarantee.

Figure 2 Big data security Model Figure 2. big data security model

4.2. Hybrid Cloud Technology

Hybrid cloud is a major model of cloud computing in recent years, and it is also the future development direction, its principle is to solve cloud computing solutions through the combination of different cloud service models. For example, the combination of public cloud and private cloud mode, in which the enterprise's public data information can be stored on the public cloud, its huge storage space and open scheme performance can provide the network customers with abundant information resources, and can create a separate private cloud behind the firewall of the enterprise, which has strong privacy, and the secrecy mechanism is far higher than that of the public cloud.

4.3. Data Search Encryption Management

Data search is a major part of the big data application, that is, the process of mining valid information, in the process of data search, will be subject to some of the security threats shown in figure 3, that is, in the search process of implanting malicious programs or stealing core data. Using encryption search technology, the data is encrypted to make the raw data change in nature, this operation makes the data search more difficult, and in the cloud storage platform, the user can search and download the data through the form of ciphertext, and then decrypt the data through the decryption tool, so that the raw data can be obtained. This technology can effectively improve the security of data information in search and reduce the possibility of privacy information infringement.

Figure 3 Data based on cloud security model Search Encryption Management

4.4. Homomorphic Cloud Encryption

Homomorphic cloud encryption technology is more secure and private than traditional encryption technology, which is characterized by the operation of data without decryption, and the results obtained after algebraic operation are still in encryption state. Therefore, using homomorphic encryption technology can solve most of the security privacy problems encountered by cloud computing process well, and also provide more possibilities for the legal and effective utilization of big data. However, this technique also has the drawback that the correctness of the calculated data cannot be verified effectively, and needs further research to improve its performance.

4.5. Anonymous Protection Technology

Anonymous protection technology is relative to data analysis and application, in data publishing, can be generalized through tuples, suppression [4]. However, in practice, data publishing has the characteristics of multiple and dynamic, so it is necessary to prevent attackers from jointly analyzing the published data. Therefore, the technology of anonymous protection is more complex and becomes the focus of big data security privacy protection research.

5. Conclusion

All in all, the wider the application of cloud computing technology, the more fragile its security performance will become, and the security problem has hampered the development of big data. At present, there is no very successful case for big data's security privacy protection for reference. In view of the emerging new security problems, we can only rely on colleagues to explore and forge ahead, develop more and better cloud security measures for cloud computing industry, make cloud service more secure and reliable, so that big data can play its effective role and promote the process of information society development.

Acknowledgements

This work is supported by the Science and Technology Plan Project of Xi’an (No. 2017CGWL35, No. 2016CXWL22, No. 2016CXWL21).

References

[1] High rain. (2019). Research on big data security and privacy protection. Wireless Internet Technology, no. 14, pp. 143-144.

[2] Tu Yunjie. (2019). Research on Data Security and Privacy Protection in Big Data Era. Wireless Internet Technology, no. 8, pp. 155-156.

[3] Wang Li. (2019). Research on big data storage security technology based on cloud computing. Information Systems Engineering, no. 5, pp. 64-64

[4] Cheng Fuxiong. (2019). Big data storage security based on cloud computing. Science and Informatization, no. 5, pp. 40-41.